

(12) UK Patent Application

(19) GB

(11) 2 221 870 (13) A

(43) Date of A publication 21.02.1990

(21) Application No 8912501.7

(22) Date of filing 31.05.1989

(30) Priority data

(31) 8812890

(32) 31.05.1988

(33) GB

(71) Applicant

The De La Rue Company Plc

(Incorporated in the United Kingdom)

**De La Rue House, 3/5 Burlington Gardens, London,
W1A 1DL, United Kingdom**

(72) Inventors

David Ezra

Theresa Hare

Peter Charles Pugsley (Deceased)

(74) Agent and/or Address for Service

Gill Jennings & Every

**53-64 Chancery Lane, London, WC2A 1HN,
United Kingdom**

(51) INT CL⁴

B42D 15/02, G06K 19/00

(52) UK CL (Edition J)

B6A AC81 ATC

U1S S2271 S2291

(56) Documents cited

GB 2108428 A US 4163570 A

(58) Field of search

UK CL (Edition J) B6A ATC

INT CL⁴ B42D 15/02, G06K 19/00

(54) **Security device**

(57) A security device comprising a substrate (1) on or in which is provided a radiation scattering structure derived from a master member (7, Fig. 3), the radiation scattering structure causing an incident, coherent beam of radiation to scatter in a random manner whereby the scattered beams interfere to generate a speckle pattern. The structure may be an embossed pattern or two transparent layers having different refractive indices. Alternatively interference effects can be created by changes of refractive index within the volume of a transmitting material.

The device is verified by comparing the speckle pattern with a reference. An auxiliary radiation scattering structure may be used to provide a composite speckle pattern.

Fig. 1.

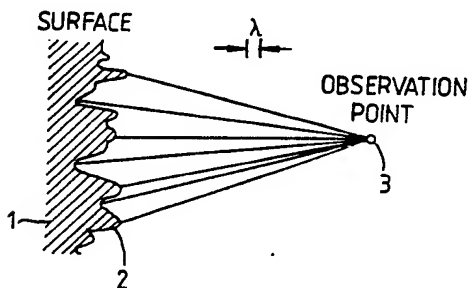
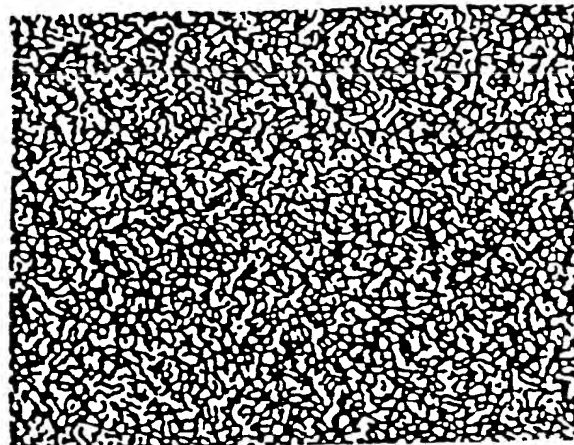


Fig. 2.



GB 2 221 870 A

1/2

2221870

Fig .1.

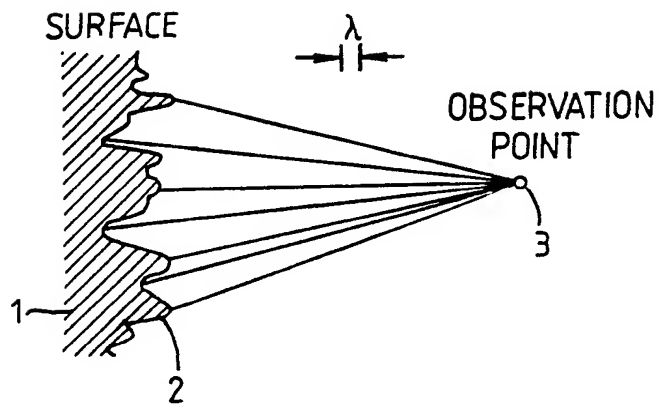


Fig .2 .

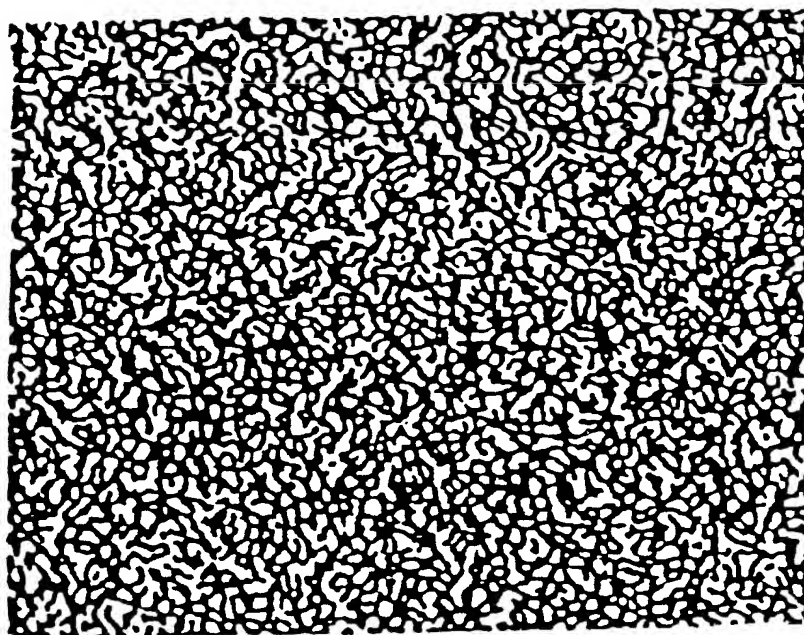


Fig .3.

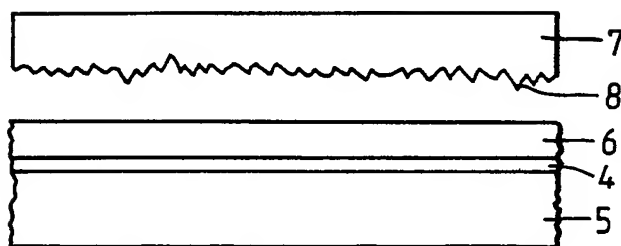
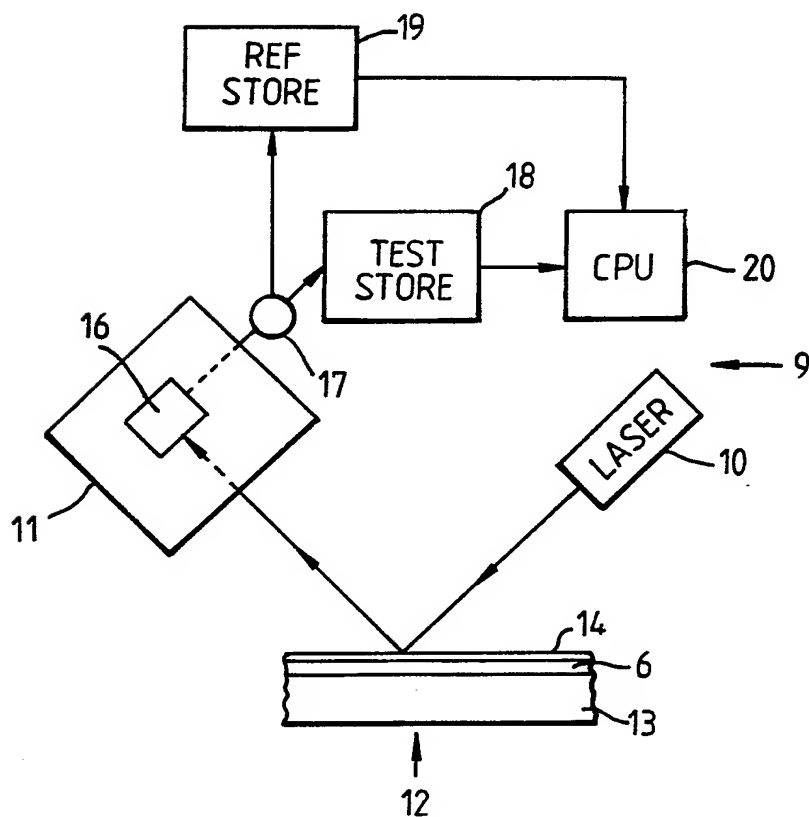


Fig .4.



SECURITY DEVICE AND METHODS AND
APPARATUS FOR VERIFICATION

5 The invention relates to a security device, for example for a label, identification card and the like and methods and apparatus for verifying such security devices.

10 Many different types of security device have been proposed in the past to prevent or reduce the risk of unauthorised copying of the article to which the device is attached. For example, various optically responsive security devices have been used such as diffraction gratings and holograms.

15 US-A-4537504 describes an authenticating feature which is a predetermined, periodic, phase profile. A random component is added in order to make it more difficult to determine the periodic structure by simple intensity measurement of the reflected light from the surface. With a partially coherent source having a
20 periodic phase profile obtained by the superposition of a (predetermined) phase diffraction grating and a randomly diffused element, the presence of the periodic phase profile can be more readily determined by measuring the degree of coherence of the scattered light than the
25 intensity thereof. However, if the measuring equipment falls into the wrong hands the periodical component (which is easy to reconstruct) can be determined and all that is needed is a random surface with similar statistical characteristics to make a replica.

30 Although these provide a reasonable degree of security, it is not impossible for the determined forger to recreate the device by reverse engineering from the pattern generated by the device when irradiated with a laser beam or by producing the original model in the case
35 of holograms.

In accordance with one aspect of the present invention, a security device comprises a substrate on or in which is provided a radiation scattering structure derived from a master member, the radiation scattering
5 structure causing an incident, coherent beam of radiation to scatter in a substantially random manner whereby the scattered beams interfere to generate a speckle pattern.

This new security device overcomes the problems of known devices by causing an incident beam to scatter in a
10 substantially random manner generating an extremely complex speckle pattern. As the phase information is lost it will be virtually impossible for a potential forger to create the initial scattering structure simply by viewing the resultant speckle interference pattern,
15 although the device itself can be mass produced from the master member. In particular it is not sufficient simply to select a surface with similar statistical characteristics. This is particularly useful where the devices are to be incorporated into security documents,
20 labels or identification cards. In the case of labels, a different scattering structure could be used for each product.

A speckle pattern for use in a label is an area of randomly varying light intensity, which gives a pattern
25 of light and dark domains of different sizes and shapes, resulting from the interference of coherent light formed by the reflecting or transmitting of that light from an (optically) unsmooth, irregular surface or through a material of varying refractive index.

30 Preferably, the radiation scattering structure is embodied in the device in such a manner that any attempt to physically access the structure will cause the structure to be destroyed. For example, the structure may be encapsulated within a suitable material, such as a

resin, whereby any attempt to remove the resin will cause the scattering structure to be destroyed.

In the preferred example, the radiation scattering structure is provided as an embossed pattern on a surface of the substrate which will normally be protected by a transparent plastic layer. In this case, the embossed pattern may be coated with a reflecting coating so that a beam incident on the embossed surface is reflected. Alternatively, the radiation scattering structure may comprise at least two transparent layers having different refractive indices, the interface between the layers being non-planar.

A further method of creating the optical interference effects is by creating changes of refractive index within the volume of a suitable transmitting material.

In order to achieve efficient or strong scattering, it is desirable that adjacent scattering centres of the scattering structure should produce scattered beams having an average phase variation greater than 2π .

In addition, the density of scattering centres in the radiation scattering structure should be high, for example between 100 and 150 scattering centres in an area defined by a 1mm diameter beam.

Typically, the radiation scattering structure will be designed to scatter a coherent radiation beam, such as a laser beam, in the visible or outside the visible wavelength range.

In accordance with a second aspect of the present invention, a method of verifying a security device according to the first aspect of the invention, comprises comparing the speckle pattern generated by the device under test with the speckle pattern generated by a reference device using the same irradiation conditions.

In accordance with a third aspect of the present invention, apparatus for verifying a security device according to the first aspect of the invention comprises a radiation generator for generating a radiation beam
5 which impinges on the radiation scattering structure of a security device under test; and comparison means for comparing the speckle pattern generated by the device under test with the speckle pattern generated by a reference device using the same illumination and
10 observation conditions.

The comparison may be achieved by making use of conventional pattern recognition techniques.

This illustrates one of the main advantages of the invention in providing a machine readable security
15 device.

For widespread use it is desirable that the device readers be portable. Thus, the preferred portable coherent radiation interfering speckle device comprises means for illuminating the specimen device with coherent
20 radiation (such as a laser diode), means for holding the device in a fixed position during illumination, means for detecting the resultant interference pattern formed by the scatter of the illumination from the device whether by transmission or reflection, means for forming
25 a series of data corresponding to the detected pattern, means for providing a series of reference data from a reference device or electronically stored reference data, means for comparing the collected data and the reference data, and means for indicating whether the comparison
30 between the collected data and the reference data falls within predetermined limits.

In a preferred arrangement, the comparison device or reader is provided with an auxiliary radiation scattering structure whereby a comparison is made between the
35 composite speckle pattern produced by the security device

under test and the auxiliary radiation scattering structure, and a reference security device and the same auxiliary radiation scattering structure. In this way, even if a counterfeiter obtains a comparison device, and
5 even if the counterfeiter is able to reverse engineer from the resultant speckle pattern the counterfeiter will only be able to produce by reverse engineering from the resultant pattern a scattering surface which produces an interference pattern which is accepted by that device.

10 The auxiliary device may be made demountable from the equipment to add a further level of security to the system. The auxiliary device may be located on a plastic card carrier which slots into the reader. The use of the auxiliary device increases the level of
15 security of the system as it renders each reader unique. This would force any counterfeiter of the surface replica to make any counterfeit to a much higher degree of precision than without it, even if the counterfeiter had a reader available.

20 The invention leads to a very cheap security device which can be relatively easily reproduced from the master and allows the same comparison device or reader to be used for any number of different radiation scattering structures. Furthermore, if a forger succeeds in
25 counterfeiting a particular security device, this does not compromise the entire system since a new radiation scattering structure can be readily produced.

The security device of the invention can be transmissive for use with tags and labels, or reflective,
30 for use as a surface mountable label.

Items containing the device include labels and tags securely attached to manufactured items, including branded goods identification tags. Such tags comprise means for securely attaching the tag to the value item.

Other items which may include the device are plastic cards including PVC cards which are widely used for a variety of purposes such as bank cards, cheque guarantee cards, cash withdrawal cards, credit cards, integrated circuit containing cards, personal identity cards, permits, and remote identification cards for physical, electronic and computer access.

Such cards typically consist of a laminate of PVC and comprise a base layer bearing a security printed layer protected by a laminate of clear PVC. Personalised information can be readily applied by using electronic recording means such as thermal printing or laser radiation induced imaging methods. Such information, to be secure, is applied to the card prior to the transparent cover sheet being laminated in place. The electronically applied personal indicia may be placed on the security printed surface which will bear the cover film, or on the underside of the film. The personal indicia may consist of one or more of the name of the holder of the card, personal reference numbers including financial account numbers, expiry dates, and representations of the signature, face or fingerprints of the holder.

The card may optionally contain a magnetic strip readable from an outer surface, preferably the strip being on the back. The card may also contain a signature strip, although graphical representations of the signature may be formed by the indication means, with this signature then being contained securely within the laminate. The card may also receive deep embossing of a further set of indicia.

The reflective speckle devices may be adhered to an outer surface of a card. The surface relief replica will be protected by a tamperproof protective layer.

The device may also be contained within the laminate, for example under the transparent covering film.

5 The device may also be integrated within another embossed pattern such as a metallised holographic or diffractive surface relief replicas, or an embossed engraving.

For example the device may be a circle of diameter 1 to 3mm contained within a surrounding diffractive graphical pattern or hologram. Alternatively it may be
10 contained within a non-optically interfering printed ring of precise diameter.

The device may be included in the metallised plastic of exposed banknote threads, or in adhesive labels for
15 affixing, for example by hot stamping means, to security based paper including banknote paper, cheque paper and the like. The device may also be included in travel tickets, admission tickets, lottery tickets, stamps, share certificates, bonds, deeds and the like.

20 An example of a security device and of a method for verifying the device in accordance with the present invention will now be described with reference to the accompanying drawings, in which:-

Figure 1 is an enlarged, partial cross-section
25 through an embossed surface of the device;

Figure 2 illustrates an example of the interference pattern produced by a device of the type shown in Figure 1;

Figure 3 is a schematic cross-section through the
30 device during an intermediate stage of manufacture; and,

Figure 4 illustrates schematically a reader for verifying a security device.

The principle of the security device is illustrated in Figure 1 which shows a substrate 1 on which is
35 embossed a random pattern 2. This causes an incident,

coherent laser beam (not shown) whether used in reflection or transmission to scatter into a multiplicity of scattered beams which, when observed at a point 3 will have travelled by a variety of different distances to that point. This means that the phase of each of the scattered beams is essentially unrelated to each other due to the random nature of the surface 2 causing a random interference pattern to be generated at the observation point. An example of this random, speckle pattern is shown in Figure 2. Figure 1 illustrates schematically the dimensions of the embossed surface relative to the wavelength λ of the incident beam. In particular, it is considered preferable if the phase variations between scattered beams from adjacent scattering centres are greater than 2π . Furthermore, the density of scattering centres should be sufficiently high to produce strong scattering and typically for an incident beam of 1mm diameter there should be between 100 and 150 scattering centres within the area of the beam.

One method of constructing the security device will now be described. Initially, a release layer 4 (Figure 3) is coated onto a polyester base layer 5. A layer of resin 6 having a thickness of about $1.5\mu\text{m}$ is coated on the release layer 4. A master embossing plate 7 carrying the required embossing pattern 8 on one surface is impressed onto the polyester composite layer so that the relief pattern 8 is embossed into the resin layer 6. The embossed resin layer 6 is coated with aluminium to provide a reflection coating and this surface is then coated with a heat sensitive adhesive. The laminate comprising layers 4-6 is mounted on a substrate (not shown) and the adhesive is activated by heat and pressure, the heat also causing the release layer 4 to melt and enabling the polyester layer 5 to be peeled away to leave the embossed, cured resin lamina 6 permanently

adhered to the substrate. The adhesive is chosen such that any attempt to separate the substrate from the embossed layer will result in destruction of the embossed surface. This prevents a forger from separating the encapsulation so as to be able to reproduce the embossed layer physically.

The embossed laminate can then be affixed to or embodied within an article to be protected, for example a label or identification card.

10 The master embossing plate 7 may be produced using a photoresist technique to create the random scattering surface followed by electroforming a replica in a hard metal such as nickel to constitute the master plate. For example, the master embossing plate 7 may be prepared
15 by selecting a random light scattering surface. Ground glass has been found to be a useful surface, possessing a usefully large number of scattering centres over an area of diameter 5mm. The surface must have a profile which causes the coherent laser radiation, which will normally
20 be visible or infrared, to be strongly scattered.

Thus typically a beam from an argon ion laser of diameter 5mm is passed orthogonally through the ground glass onto the surface of a photoresist, positioned broadly in parallel with the resist at a distance of
25 about 1000mm. The emission of the laser is chosen so as to match the sensitivity of the resist. A 10mm beam at a distance of 2000mm will give similar results.

The beam exposes the resist surface, covering an area very much larger than the beam diameter. Using
30 the above parameters the speckle pattern on the resist will have an autocorrelation length of about 0.1mm, thus ensuring an adequate number of scattering centres when portions of the resist replicas of diameter about 1mm are selected for the final labels.

In general the autocorrelation length of the speckle is proportional to the wavelength of the laser and the distance between the glass and resist planes, and inversely proportional to the diameter of the illuminated area of the incident laser beam. These geometrical parameters also contribute to the arrangement of the final pattern. Thus the surface profile is dependent on the ground glass surface and the optical geometry.

The photoresist is developed in the normal manner to reveal a surface profile. This profile will have a depth of at least 1 micron. The resist is then electroplated with nickel in the conventional manner and removed. The resulting nickel replica may then be used to form further (although reversed) replicas if necessary. The first or second surface relief nickel replica is then used to form a replica in plastic, for example by hot embossing (as described above) or by casting or curing. Portions of the final surface relief plastic replica are then used as the unique speckle generating labels. Typically a portion of diameter about 1mm will be used in a tag or label. The surface profile in the plastic may be metallised for reflectivity.

In order to verify a security device of this type, a label reader 9 is provided comprising a laser 10 (which for example may generate a beam with a wavelength of 780nm) and a reading device 11. The label 12 is brought into alignment with the laser beam as shown in Figure 4 with the embossed layer 6 mounted on the main body 13 of the label and carrying the encapsulation layer 14. The incident laser beam is scattered, as previously described, and the scattered beam generates a speckle pattern which is received in the reading device 11. The speckle, interference pattern is then detected using a conventional detector 16, such as a charge coupled

device, positioned about 100mm from the label which digitises the received pattern and passes the digital version via a switch 17 to a test store 18. A series of data points corresponding to picture elements (pixels) of the CCD array may be collected. The resulting data may simply record two illumination levels, that is light and dark, with intermediate values being disregarded. Alternatively the data may record various levels of light intensity.

By using different portions of the photoresist surface a range of unique patterns can be obtained. These patterns when cast in plastic can be used as individual items or alternatively multiples can be made.

Counterfeiting by reproducing an optically interfering surface which gives identical unique patterns is almost impossible just by observing the light intensity distribution as the phase information of the surface is lost.

In a similar manner, a reference device with which the test device is to be verified is placed in the same position as the test device and illuminated in a similar manner, the digitised version being stored in a reference store 19. A microcomputer 20 then compares the patterns in the test and reference stores 18, 19 using a conventional comparison technique and providing there is sufficient similarity, indicates that the test device is verified as a true device.

The sample and the reference may differ slightly in their absolute position relative to the image recognising optics. Minor differences can be overcome by computational techniques, for example such as those which are used for fingerprint verification described in GB 2174831B.

The combination of the speckle device with reference points located close to the outside of the device allows

the optical system to accommodate orientation and absolute location differences more readily. The optical system may then use these location points to calculate the orientation of the device before making the
5 comparison. Such a method allows time saving and reduced computing capacity.

Typically, the dimensions of the security device will be about 2mm x 2mm while the diameter of the laser beam will be about 2mm.

10 Although the scattering structure has been described as constituting a complete security device, it could form part of a larger security device in order to reduce the possibility of such a device being fraudulently reproduced.

15

20

25

30

35

CLAIMS

1. A security device comprising a substrate on or in which is provided a radiation scattering structure
5 derived from a master member, the radiation scattering structure causing an incident, coherent beam of radiation to scatter in a substantially random manner whereby the scattered beams interfere to generate a speckle pattern.
2. A device according to claim 1, wherein the radiation
10 scattering structure is embodied in the device in such a manner that any attempt to physically access the structure will cause the structure to be destroyed.
3. A device according to claim 1 or claim 2, wherein the radiation scattering structure is provided as an
15 embossed pattern on a surface of the substrate.
4. A device according to claim 1 or claim 2, wherein the radiation scattering structure comprises at least two transparent layers having different refractive indices, the interface between the layers being non-planar.
- 20 5. A device according to any of the preceding claims, wherein the radiation scattering structure scatters a coherent optical beam of radiation.
6. An identification card incorporating a security device according to any of the preceding claims.
- 25 7. A security document incorporating a security device according to any of claims 1 to 5.
8. A method of verifying a security device according to any of claims 1 to 5, the method comprising comparing the speckle pattern generated by the device under test
30 with the speckle pattern generated by a reference device using the same irradiation conditions.
9. Apparatus for verifying a security device according to any of claims 1 to 5, the apparatus comprising a radiation generator for generating a radiation beam which
35 impinges on the radiation scattering structure of a

security device under test; and comparison means for
comparing the speckle pattern generated by the device
under test with the speckle pattern generated by a
reference device using the same illumination and
5 observation conditions.

10. Apparatus according to claim 9, further comprising
an auxiliary radiation scattering structure whereby a
comparison is made between the composite speckle pattern
produced by the security device under test and the
10 auxiliary radiation scattering structure, and a reference
security device and the same auxiliary radiation
scattering structure.

15

20

25

30

35